目　次

まえがき

1　公開鍵暗号システムがあぶない・・・・・・・・・・・1

2　理想の暗号・・・・・・・・・・・・・・・・・・・・・・・4

2.1　第二次大戦と近代暗号　4

2.2　暗号文の作成　5

2.3　落し戸関数　7

2.4　使い捨てパッド方式　9

3　公開鍵暗号の安全性・・・・・・・・・・・・・・・・・13

3.1　公開鍵暗号　13

3.2　古典的コンピュータによる暗号解読　17

4　量子コンピュータ・・・・・・・・・・・・・・・・・・・22

4.1　量子チューリング機械　23

4.2　量子並列計算　26

4.3　計算木　28

4.4　量子回路　31

5　量子コンピュータによる暗号解読・・・・・・・・38

5.1　ショアのアルゴリズムの概要　40

5.2　ショアのアルゴリズムの詳細　43

5.3　計算機シミュレーション　49

6　量子暗号・・・・・・・・・・・・・・・・・・・・・・・・52

6.1　破られない暗号はあるか　53

6.2 暗号の盗聴者の発見 56
6.3 量子暗号のこれから 57

7 量子コンピュータの実現法 ・・・・・・・・・・・・ 60
7.1 物理的に実現するには 60
7.2 ヘテロポリマー量子コンピュータ 61
7.3 イオントラップ量子コンピュータ 62
7.4 キャビティ QED 量子コンピュータ 64
7.5 NMR 量子コンピュータ 65

8 おわりに——基礎研究の重要性・・・・・・・・・・・・・ 68

あとがき 73
索 引 77